Your IC3 Complaint

Submission ID:	300f8553ba11406383fdfb2986558f07
Date Filed:	3/29/2025 6:13:21 PM EST
Were you the one affected in this incident?	Yes

Your Contact Information

Name:	John R. Fouts
Phone Number:	5029560052
Email Address:	fouts.john@gmail.com

Complainant Information

Name:	John R. Fouts
Age:	40 - 49
Address:	2904 Sitka Dr.
Suite/Apt./Mail Stop:	L29
City:	Louisville
Country:	United States of America
State:	Kentucky
Zip Code/Route:	40299
Phone Number:	5029560052
Email Address:	fouts.john@gmail.com

Business Information

Is this on behalf of a business that was targeted by a Cyber incident?	No

Financial Transaction(s)

Did you send or lose money in the incident?	Yes
What was your total loss amount?	3,850.00
Transaction Type:	Other
If other, please specify:	Cyber Intrusion Expenses & Surveillance Countermea
Was the money sent or lost?	Yes
Transaction Amount:	3,850.00
Transaction Date:	03/29/2025
Did you contact your bank, financial institution, or cryptocurrency exchange?	No

Information About The Subject(s)

Name:	Xiber LLC
Business Name:	Xiber Networks
Address:	Xiber LLC
Address (continued):	20 E 91st St #200,
City:	Indianapolis
Country:	United States of America
State:	Indiana
Zip Code/Route:	46204
Phone Number:	3176442240
Email Address:	amy@xiber.on.crisp.email
Website/Social Media Account:	https://www.xiber.net
IP Address	104.251.168.1

Description of Incident

Provide a description of the incident and how you (or those you are filling this out on behalf of) were victimized. Provide information not captured elsewhere in this complaint form:

Between March 15 and March 28, 2025, I began observing signs of a potential advanced persistent threat (APT) or malicious remote access activity on my home network.

While connected to Xiber Internet Services (static IP via passthrough mode, IP block 104.251.168.x, based in Indianapolis), I experienced:

Unexpected Google account logins showing IP addresses in Ireland (54.217.128.108 / 54.217.125.108) despite no VPN usage at the time

Frequent ICMP “Port Unreachable” messages on localhost (127.0.0.1)

Suspicious virtual adapter behavior (e.g., 192.168.137.x)

Unexpected system behavior and persistent tracking even behind firewall, hardened browser, and VPN

I contacted Xiber multiple times, requesting log reviews and specific traces of the Ireland-originating IP. They declined to provide logs and failed to answer whether any external traffic had tunneled through their infrastructure or reached my assigned address.

I believe either:

Their infrastructure has been compromised or misconfigured in a way that allowed this access

A rogue insider or external attacker is leveraging their NAT policies for obfuscation

Their silence is intentional, obstructive, or influenced by a third party

The situation has caused extreme distress, forced me to expend funds on advanced detection tools, and complicated ongoing legal proceedings that depend on digital integrity. I am requesting federal review of this provider and their security posture.

Other Information

If an email was used in this incident, please provide a copy of the entire email including full email headers.

• Observed unauthorized login to Google account from IP 54.217.125.108 and 54.217.128.108 (Amazon AWS Ireland) — I was not connected to VPN or outside the U.S. at the time.
• My static IP address from ISP (Xiber) is 104.251.168.33, in Louisville, KY.
• Xiber is routing via NAT; I have requested connection logs and IP routing logs but

they have refused to provide them.
• Persistent tracking even behind VPN, hardened browser, anti-fingerprinting.
• Localhost ICMP Port Unreachable messages seen in Wireshark, looping, indicating spoofed or internal misrouted traffic.
• Unusual WMI EventConsumers and Scheduled Tasks have been found and cleared.
• “ShadowSentinel” custom PowerShell tool was deployed to monitor real-time attacks, but attempts to run it were blocked, suggesting anti-forensic measures in play.
• Evidence includes screenshots, Google login timestamp, PowerShell monitoring output, and logs from defender/honeypot alerts.
• Unable to access or run forensic tools reliably, possibly due to sabotage or implant interference.

Are there any other witnesses or persons affected by this incident?

Yes. My child and I are both affected. We share the same network and systems and have experienced similar signs of intrusion. This may be tied to larger systemic targeting as part of ongoing legal and civil rights claims. I am documenting evidence for both of us.

If you have reported this incident to other law enforcement or government agencies, please provide the name, phone number, email, date reported, report number, etc.

Yes. I have sent multiple reports to my ISP (Xiber) including formal requests for logs and investigation, which have been ignored or answered vaguely. Also preparing documentation for DOJ Civil Rights, HHS OCR, and FCC regarding access, abuse, and surveillance implications. Additional complaints pending to Kentucky State agencies and internal security divisions of Google and Microsoft.

Is this an update to a previously filed complaint? No

Privacy & Signature:

The collection of information on this form is authorized by one or more of the following statutes: 18 U.S.C. § 1028 (false documents and identity theft); 1028A (aggravated identity theft); 18 U.S.C. § 1029 (credit card fraud); 18 U.S.C. § 1030 (computer fraud); 18 U.S.C. § 1343 (wire fraud); 18 U.S.C 2318B (counterfeit and illicit labels); 18 U.S.C. § 2319 (violation of intellectual property rights); 28 U.S.C. § 533 (FBI authorized to investigate violations of federal law for which it has primary investigative jurisdiction); and 28 U.S.C. § 534 (FBI authorized to collect and maintain identification, criminal information, crime, and other records).

The collection of this information is relevant and necessary to document and investigate complaints of Internet-related crime. Submission of the information

requested is voluntary; however, your failure to supply requested information may impede or preclude the investigation of your complaint by law enforcement agencies.

The information collected is maintained in one or more of the following Privacy Act Systems of Records: the FBI Central Records System, Justice/FBI-002, notice of which was published in the Federal Register at 63 Fed. Reg. 8671 (Feb. 20, 1998); the FBI Data Warehouse System, DOJ/FBI-022, notice of which was published in the Federal Register at 77 Fed. Reg. 40631 (July 10, 2012). Descriptions of these systems may also be found at www.justice.gov/opcl/doj-systems-records#FBI. The information collected may be disclosed in accordance with the routine uses referenced in those notices or as otherwise permitted by law. For example, in accordance with those routine uses, in certain circumstances, the FBI may disclose information from your complaint to appropriate criminal, civil, or regulatory law enforcement authorities (whether federal, state, local, territorial, tribal, foreign, or international). Information also may be disclosed as a routine use to an organization or individual in both the public or private sector if deemed necessary to elicit information or cooperation from the recipient for use by the FBI in the performance of an authorized activity. "An example would be where the activities of an individual are disclosed to a member of the public in order to elicit his/her assistance in [FBI's] apprehension or detection efforts." 63 Fed. Reg. 8671, 8682 (February 20, 1998).

By typing my name below, I understand and agree that this form of electronic signature has the same legal force and effect as a manual signature. I affirm that the information I provided is true and accurate to the best of my knowledge. I understand that providing false information could make me subject to fine, imprisonment, or both. (Title 18, U.S.Code, Section 1001)

Digital Signature: John R. Fouts